

(19) 世界知的所有権機関  
国際事務局



(43) 国際公開日  
2002 年 4 月 25 日 (25.04.2002)

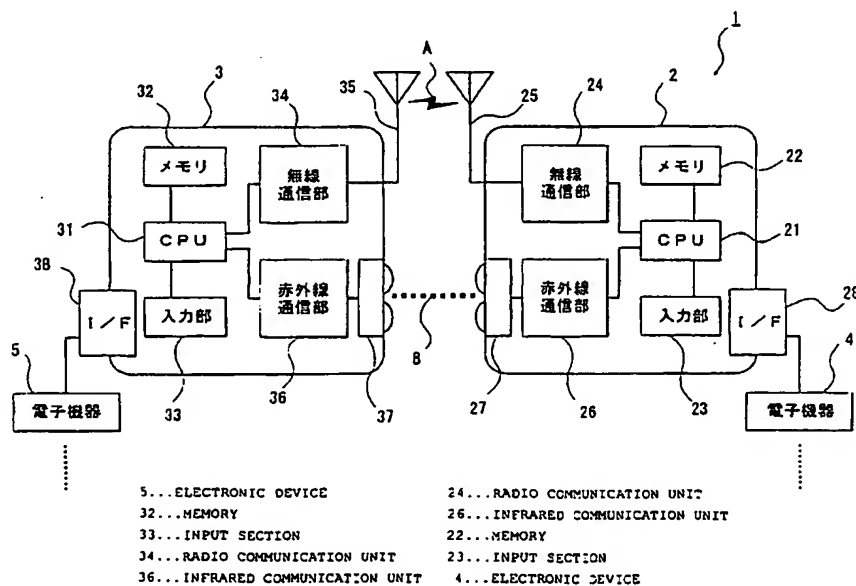
PCT

(10) 国際公開番号  
WO 02/33905 A1

- (51) 国際特許分類<sup>7</sup>: H04L 12/28 (KITAZUMI, Gontaro) [JP/JP]; 〒156-0043 東京都世田谷区松原三丁目40番7号 リンク・エボリューション株式会社内 Tokyo (JP).
- (21) 国際出願番号: PCT/JP01/04441
- (22) 国際出願日: 2001 年 5 月 28 日 (28.05.2001)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:  
特願 2000-315395  
2000 年 10 月 16 日 (16.10.2000) JP
- (71) 出願人 (米国を除く全ての指定国について): リンク・エボリューション株式会社 (LINK EVOLUTION CO., LTD) [JP/JP]; 〒156-0043 東京都世田谷区松原三丁目40番7号 Tokyo (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 北角 権太郎
- (74) 代理人: 荒船博司, 外 (ARAFUNE, Hiroshi et al.); 〒162-0832 東京都新宿区岩戸町18番地 日交神楽坂ビル5階 Tokyo (JP).
- (81) 指定国 (国内): US.
- (84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).
- 添付公開書類:  
— 国際調査報告書
- 2 文字コード及び他の略語については、定期発行される各 PCT ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(54) Title: COMMUNICATION APPARATUS, COMMUNICATION SYSTEM AND COMMUNICATION METHOD

(54) 発明の名称: 通信装置、通信システム及び通信方法



(57) Abstract: A communication apparatus comprising first communication means for transmitting/receiving radio signals; second communication means for transmitting/receiving signals by use of a communication system that is different from the communication system of the first communication means; key information holding means for holding encryption key information; key information transmission control means for causing the second communication means to transmit the encryption key information held in the key information holding means to another communication apparatus; and communication control means for encrypting information on the basis of the encryption key information held in the key information holding

[続葉有]



---

means and for causing the first communication means to transmit the encrypted information. In a case of transmitting/receiving data by means of radio communications among a plurality of electronic devices, the reliability of security can be enhanced without degrading the facility of the radio communications.

(57) 要約:

無線信号を送受信する第1の通信手段と、この第1の通信手段とは異なる通信方式により信号を送受信する第2の通信手段と、暗号化鍵情報を保持する鍵情報保持手段と、この鍵情報保持手段に保持された暗号化鍵情報を、前記第2の通信手段によって他の通信装置へ送信させる鍵情報送信制御手段と、前記鍵情報保持手段に保持された暗号化鍵情報をもとに情報を暗号化して、前記第1の通信手段によって送信させる通信制御手段とを備える通信装置。複数の電子機器間で無線通信によってデータを送受信する場合に、無線通信の利便性を損なうことなくセキュリティ上の信頼性を向上させることができる。

## 明 細 書

## 通信装置、通信システム及び通信方法

## 5 技術分野

本発明は、異なる複数の通信方式に対応する通信装置、この通信装置を備える通信システム及びこの通信システムにおける通信方法に関する。

## 背景技術

- 10 従来、パーソナルコンピュータ、PDA (Personal Digital Assistant)、携帯電話機等の電子機器間でデータ通信を行う場合には、互いの電子機器をケーブルで接続する手法が用いられていた。しかし、ケーブルを用いた手法は、電子機器にケーブルを接続する手間がかかり、ケーブルを携帯しなければならないため、不便であった。そこで、最近では、複数の電子機器間におけるデータ
- 15 通信に無線通信技術が用いられるようになった。

特に、近年では、電子機器の利便性を向上させるため、互換性に富む複数の無線通信規格が策定されている。これらの通信規格に準じた通信装置を用いれば、様々な電子機器との間でデータ通信を容易に行うことができる。

- しかしながら、無線通信技術を利用してデータ通信を行う場合は、データの漏洩に注意する必要がある。特に、様々な機器との間で通信可能な通信規格に準じている場合は、誤って無関係な他の機器によってデータが受信されないように注意する必要がある。このように、無線通信技術を用いたデータ通信では、セキュリティ上の信頼性を向上することが課題となっていた。
- 20

- 本発明の課題は、複数の電子機器間で無線通信によってデータを送受信する場合に、無線通信の利便性を損なうことなくセキュリティ上の信頼性を向上させることである。
- 25

## 発明の開示

本発明は、このような課題を解決するために、次のような特徴を備えている。

なお、次に示す手段の説明中、括弧書きにより実施の形態に対応する構成を一例として示す。符号等は、後述する図面参照符号等である。

本発明の第１の側面によれば、この通信装置（２）は、

無線信号を送受信する第１の通信手段（例えば、図１に示す無線通信部２４）

５ と、

この第１の通信手段とは異なる通信方式により信号を送受信する第２の通信手段（例えば、図１に示す赤外線通信部２６）と、

暗号化鍵情報を保持する鍵情報保持手段（例えば、図２に示す原始暗号化情報格納領域１０１を有するメモリ２２）と、

10 この鍵情報保持手段に保持された暗号化鍵情報を、前記第２の通信手段によって他の通信装置へ送信させる鍵情報送信制御手段（例えば、図３に示す処理を行うＣＰＵ２１）と、

前記鍵情報保持手段に保持された暗号化鍵情報をもとに情報を暗号化して、前記第１の通信手段によって送信させる通信制御手段（例えば、図５に示す処理を行うＣＰＵ２１）とを備える。

15 このような構成を備えた本発明の通信装置によれば、無線信号を送受信する第１の通信手段と、この第１の通信手段とは異なる通信方式により信号を送受信する第２の通信手段とを備え、鍵情報保持手段により、暗号化鍵情報を保持し、この鍵情報保持手段に保持された暗号化鍵情報を、鍵情報送信制御手段の  
20 制御により、第２の通信手段によって他の通信装置へ送信するとともに、通信制御手段の制御によって、鍵情報保持手段に保持された暗号化鍵情報をもとに情報を暗号化して、第１の通信手段によって送信するので、この通信装置により送信される情報は、第２の通信手段によって送信された暗号化鍵情報を受信した通信装置でのみ受信することができる。これにより、第１の通信手段による無線通信について、セキュリティ上の信頼性を確保することができる。特に、  
25 第１の通信手段による無線通信が、例えばブルートゥース規格のように、仕様や規格が公開され、或いは広く普及して互換性が保たれている無線通信方式に準じたものである場合は、無関係な通信装置により情報が受信されてしまう可能性が否定できない。しかしながら、本発明を適用すれば、通信の相手を、第

2の通信手段によって送信される暗号化鍵情報を受信した通信装置のみに限定できる。従って、通信相手の装置との位置関係が比較的自由である等、無線通信の利便性を損なうことなく、情報の秘匿性を保持し、セキュリティ上の信頼性を確保することができる。

- 5 本発明の通信装置において、好ましくは、前記鍵情報保持手段に保持された暗号化鍵情報と同一の暗号化鍵情報を保持していない外部の通信装置に対しては、前記第1の通信手段による無線信号の送受信を拒否する通信拒否手段（例えば、図5のステップS45に示す処理を行うCPU21）をさらに備える。

このような構成の通信装置によれば、鍵情報保持手段に保持された暗号化鍵  
10 情報と同一の暗号化鍵情報を保持していない外部の通信装置に対しては、通信拒否手段により、第1の通信手段による無線信号の送受信を拒否するので、通信の相手となる通信装置を厳格に限定し、情報の秘匿をより確実に保持することができる。

- また、上記通信装置において、前記第1の通信手段はブルートゥース  
15 (Bluetooth) 規格に準じた通信方式により無線信号を送受信するものであり、前記第2の通信手段は、赤外線信号を用いた通信方式により無線信号を送受信するものとしてもよい。

このような構成の通信装置によれば、第1の通信手段はブルートゥース  
(Bluetooth) 規格に準じた通信方式により無線信号を送受信するものであり、  
20 第2の通信手段は、赤外線信号を用いた通信方式により無線信号を送受信するので、広く仕様が公開され、利便性に富む一方、確実な情報秘匿が困難なブルートゥース (Bluetooth) 規格の無線通信において、情報の秘匿性を確保することができる。特に、第2の通信手段に赤外線信号を用いた通信方式を利用するので、第2の通信手段の小型化、軽量化、低コスト化および省電力化が可能で  
25 あり、容易に実現可能である。また、赤外線信号を用いた通信方式では、通信装置は互いに近接し、かつ所定の立体角以内で対向する必要があるので、情報の秘匿性をより一層高めることができる。

本発明の第2の側面によれば、この通信システムは、

送信側装置（例えば、図 1 に示す通信装置 2）と受信側装置（例えば、図 1 に示す通信装置 3）とを備えてなる通信システム（1）であって、

前記送信側装置は、

無線信号を送受信する第 1 の通信手段（例えば、図 1 に示す無線通信部 2 4）

5 と、

この第 1 の通信手段とは異なる通信方式により信号を送受信する第 2 の通信手段（例えば、図 1 に示す赤外線通信部 2 6）と、

暗号化鍵情報を保持する鍵情報保持手段（例えば、図 2 に示す原始暗号化情報格納領域 1 0 1 を有するメモリ 2 2）と、

10 この鍵情報保持手段に保持された暗号化鍵情報を、前記第 2 の通信手段によって前記受信側装置へ送信させる鍵情報送信制御手段（例えば、図 3（a）に示す処理を行う CPU 2 1）と、

前記鍵情報保持手段に保持された暗号化鍵情報をもとに情報を暗号化して、前記第 1 の通信手段によって前記受信側装置へ送信させる通信制御手段（例え

15 ば、図 5 に示す処理を行う CPU 2 1）とを備え、

前記受信側装置は、

前記送信側装置が有する第 2 の通信手段により送信された暗号化鍵情報を受信する鍵情報受信手段（例えば、図 1 に示す赤外線通信部 3 6、及び図 3（b）に示す処理を行う CPU 3 1）と、

20 この鍵情報受信手段により受信された暗号化鍵情報を保持する受信鍵情報保持手段（例えば、図 1 に示すメモリ 3 2）と、

前記送信側装置が有する第 1 の通信手段により送信された情報を受信する暗号化情報受信手段（例えば、図 1 に示す無線通信部 3 4）とを備える。

25 このような構成を備えた本発明の通信システムによれば、送信側装置と受信側装置とを備えてなる通信システムであって、送信側装置は、無線信号を送受信する第 1 の通信手段と、この第 1 の通信手段とは異なる通信方式により信号を送受信する第 2 の通信手段とを備え、鍵情報保持手段により暗号化鍵情報を保持し、鍵情報保持手段に保持された暗号化鍵情報を、鍵情報送信制御手段によって、第 2 の通信手段によって受信側装置へ送信させるとともに、通信制御

- 手段の制御によって、鍵情報保持手段に保持された暗号化鍵情報をもとに情報を暗号化して、第 1 の通信手段によって受信側装置へ送信し、受信側装置は、送信側装置が有する第 2 の通信手段により送信された暗号化鍵情報を鍵情報受信手段によって受信し、鍵情報受信手段により受信された暗号化鍵情報を受信
- 5 鍵情報保持手段によって保持し、送信側装置が有する第 1 の通信手段により送信された情報を暗号化情報受信手段によって受信する。

また、本発明の第 3 の側面によれば、この通信方法は、

- 無線信号を送受信する第 1 の通信手段（例えば、図 1 に示す無線通信部 2 4）
- 10 と、この第 1 の通信手段とは異なる通信方式により信号を送受信する第 2 の通信手段（例えば、図 1 に示す赤外線通信部 2 6）とを有する送信側装置（例えば、図 1 に示す通信装置 2）と、受信側装置（例えば、図 1 に示す通信装置 3）とを備えてなる通信システム（1）における通信方法であって、

- 前記送信側装置により、暗号化鍵情報を前記第 2 の通信手段によって前記受信側装置へ送信する工程と、
- 15

前記受信側装置により、前記送信側装置が有する第 2 の通信手段により送信された暗号化鍵情報を受信して記憶する工程と、

前記送信側装置により、前記暗号化鍵情報をもとに情報を暗号化して、前記第 1 の通信手段によって前記受信側装置へ送信する工程とを含む。

- 20 従って、この通信方法によれば、送信側装置により送信される情報は受信側装置でのみ受信することができる。これにより、送信側装置が有する第 1 の通信手段を用いた通信システム内の無線通信について、セキュリティ上の信頼性を確保することができる。特に、第 1 の通信手段による無線通信が、例えばブルートゥース規格のように、仕様や規格が公開され、或いは広く普及して互換性が保たれている無線通信方式に準じたものである場合は、無関係な通信装置
- 25 により受信されてしまう可能性が否定できない。しかしながら、本発明を適用すれば、通信の相手を、第 2 の通信手段によって送信される暗号化鍵情報を保持する受信側装置のみに限定できる。従って、互いの装置の位置関係が比較的自由である等、無線通信の利便性を損なうことなく、情報の秘匿性を保持し、

セキュリティ上の信頼性を確保することができる。

上記通信システムまたは上記通信方法において、

前記送信側装置は、前記鍵情報保持手段に保持された暗号化鍵情報と同一の  
5 暗号化鍵情報が、前記受信側装置が有する受信鍵情報保持手段に保持されてい  
ない場合に、前記第 1 の通信手段による無線信号の送受信を拒否する通信拒否  
手段（例えば、図 5 のステップ S 4 5 に示す処理を行う CPU 2 1）をさらに  
備えるようにしてもよい。

このような構成とすれば、送信側装置は、鍵情報保持手段に保持された暗号  
10 化鍵情報と同一の暗号化鍵情報が、受信側装置が有する受信鍵情報保持手段に  
保持されていない場合に、通信拒否手段によって、第 1 の通信手段による無線  
信号の送受信を拒否するので、通信の相手となる通信装置をより厳格に限定し、  
情報の秘匿をより確実に保持することができる。

15 また、上記通信システムまたは上記通信方法において、

前記送信側装置が有する第 1 の通信手段と、前記受信側装置が有する暗号化  
情報受信手段とは、ブルートゥース (Bluetooth) 規格に準じた通信方式により  
無線信号を送受信するものであって、

前記送信側装置が有する前記第 2 の通信手段と、前記受信側装置が有する鍵  
20 情報受信手段とは、赤外線信号を用いた通信方式により無線信号を送受信する  
ようにしてもよい。

このようにすれば、送信側装置が有する第 1 の通信手段と、受信側装置が有  
する暗号化情報受信手段とは、ブルートゥース (Bluetooth) 規格に準じた通信  
方式により無線信号を送受信するものであって、送信側装置が有する第 2 の通  
25 信手段と、受信側装置が有する鍵情報受信手段とは、赤外線信号を用いた通信  
方式により無線信号を送受信するので、広く仕様が公開され、利便性に富む一  
方、確実な情報秘匿が困難なブルートゥース (Bluetooth) 規格の無線通信にお  
いて、情報の秘匿性を確保することができる。特に、第 2 の通信手段と鍵情報  
受信手段とは赤外線信号を用いた通信方式を利用するので、第 2 の通信手段お



よび鍵情報受信手段の小型化、軽量化、低コスト化および省電力化が可能であり、容易に実現可能である。また、赤外線信号を用いた通信方式では、送信側装置と受信側装置とは互いに近接し、かつ所定の立体角以内で対向する必要があるため、情報の秘匿性をより一層高めることができる。

- 5      また、前記送信側装置が有する鍵情報送信制御手段は、前記暗号化鍵情報を暗号化して前記第2の通信手段によって送信させるようにしてもよい。

そうすれば、送信側装置が有する鍵情報送信制御手段は、暗号化鍵情報を暗号化して第2の通信手段によって送信させるので、暗号化鍵情報を送信する際の情報の漏洩をより確実に防止できる。これにより、セキュリティ上の信頼性をより一層高めることができる。

10

#### 図面の簡単な説明

図1は、本発明を適用した第1の実施の形態における通信システム1の構成を示すブロック図、

- 15      図2は図1のメモリ22、32の内部構成を模式的に示す図、

図3は、図1の通信装置2および通信装置3の動作を示すフローチャート、

- 図4Aおよび4Bは、図3に示す処理に暗号化を施した場合のプロトコル構成を示す説明図であり、図4Aは暗号化を施す際の赤外線通信におけるプロトコル構成を示す階層モデル、図4Bは赤外線通信におけるデータユニットの構成を模式的に示し、
- 20

図5は、図1の通信装置2によりBluetooth規格に準じた無線通信を行う際の動作を示すフローチャート、

図6は、本発明を適用した第2の実施の形態における通信システム10の構成を示すブロック図、

- 25      図7は、図6に示すメモリ61の内部構成を模式的に示す図である。

#### 発明を実施するための最良の形態

以下、図を参照して本発明の実施の形態を詳細に説明する。

第1の実施の形態：

図 1 は、本発明を適用した第 1 の実施の形態としての通信システム 1 の構成を示すブロック図である。同図に示すように、通信システム 1 は、互いに通信可能な通信装置 2 及び通信装置 3 により構成される。通信装置 2 と通信装置 3 との間には、無線電波を媒体とする無線通信リンク A と、赤外線を利用した赤外線通信リンク B とが形成される。

なお、図 1 に示す通信装置 2 及び通信装置 3 は、いずれも同一構成によってなる通信装置であるが、本第 1 の実施の形態においては、通信装置 2 をアクセス要求側の装置、通信装置 3 をアクセス受信側の装置として説明する。

通信装置 2 は、CPU (Central Processing Unit) 21、メモリ 22、入力部 23、無線通信部 24、アンテナ 25、赤外線通信部 26、赤外線受発光ユニット 27、及びインターフェース部 28 の各部を備えて構成される。

CPU 21 は、入力部 23 における指示操作に従って、メモリ 22 に格納されたシステムプログラムを読み出して実行し、通信装置 2 の各部を駆動制御する。

具体的には、CPU 21 は、メモリ 22 内のプログラムに従って、無線通信部 24 を制御し、通信装置 3 との間に無線通信リンク A を確立する。続いて CPU 21 は、赤外線通信部 26 及び赤外線受発光ユニット 27 によって赤外線通信リンク B を確立する。そして、CPU 21 は、赤外線通信リンク B を介して、メモリ 22 内に格納された暗号化に関する各種情報を通信装置 3 へ送信する。

その後、CPU 21 は、通信装置 3 から赤外線通信リンク B を介して送信された情報を受信し、情報の内容を確認して、通信装置 3 との間の無線通信リンク A 及び赤外線通信リンク B を切断する。

また、CPU 21 は、入力部 23 から入力される指示に従って、無線通信部 24 を制御し、通信装置 2 の近辺に存在する通信装置をスキャンするための無線信号をアンテナ 25 から出力させる。このスキャン動作により、無線通信回線を介して接続可能な通信装置が検出された場合には、検出された通信装置から送信された情報を無線通信部 24 によって受信して解析する。

そして、受信した情報をメモリ 22 内に格納された原始暗号化情報と照合し、

一致した場合には接続を許可して、該検出された通信装置との間で無線通信を開始する。また、受信した情報が原始暗号化情報と一致しない場合には、該通信装置との間の通信を拒否する。

メモリ 22 は、EEPROM、フラッシュメモリ等の不揮発性記憶素子を備えて構成される。メモリ 22 は、CPU 21 により実行されるシステムプログラム等のプログラム及びこれらプログラムに係るデータ等を格納する。

また、メモリ 22 は、CPU 21 により処理されるデータや、入力部 23 から入力されたデータ等を一時的に保持する。

10      ここで、メモリ 22 に格納されるデータについて説明する。

図 2 は、メモリ 22 内部の構成を模式的に示す図である。メモリ 22 内には、上記各種プログラムを格納した格納領域（図示略）の他、図 2 に示すように原始暗号化情報格納領域 101 及び転送諸元情報格納領域 102 が設けられる。

原始暗号化情報格納領域 101 には、暗号化の際の「鍵」として使用される暗号化鍵情報、及び、暗号化鍵情報を他の電子機器に対して送信した履歴等を含む暗号化鍵管理情報が格納される。原始暗号化情報格納領域 101 に格納される各種情報を、原始暗号化情報と総称する。

この原始暗号化情報格納領域 101 に格納される原始暗号化情報は、予め原始暗号化情報格納領域 101 に格納されているものとしても良いし、入力部 23 の操作によって、随時入力されるようにしても良い。

また、転送諸元情報格納領域 102 には、通信装置 2 の製品情報、固有機能情報、使用者情報、シリアル No. 等の各種情報が格納される。これらの転送諸元情報格納領域 102 に格納される各種情報を、転送諸元情報と総称する。

なお、転送諸元情報格納領域 102 に格納される情報は、予めメモリ 22 に格納されているものとしても良いし、入力部 23 の操作によって入力されるものとしても良く、或いは、インターフェース部 28 に接続された電子機器 4 から入力されるものとしても良い。

入力部 23 は、それぞれ入力可能な情報が割り当てられた複数のキー等の入力デバイスを備えており、操作内容に対応する操作信号を生成して CPU 21

へ出力する。

無線通信部 24 は、エンコーダ、デコーダ、RF、アンプ等を内蔵しており、CPU 21 から入力される信号を変換して無線信号を生成し、アンテナ 25 を介して通信装置 3 へ送信する。また、無線通信部 24 は、通信装置 3 から送信された無線信号をアンテナ 25 によって受信し、受信した無線信号を変換して得られる信号を CPU 21 へ出力する。

ここで、無線通信部 24 としては、例えば、ブルートゥース (Bluetooth) 規格に準じた無線通信ユニットが挙げられる。

Bluetooth 規格とは、通信機器、電子機器、ソフトウェア等を製造する事業者が複数集まって構成されるプロモーターと、Bluetooth SIG (Special Interest Group) により策定された無線通信規格である。Bluetooth 規格では、2.4GHz (ギガヘルツ) 帯の周波数の無線信号を利用して、およそ数メートル以内の複数の電子機器間で無線通信を行う。

Bluetooth 規格に準じた無線通信ユニットを搭載した電子機器は、互いにピコネットと呼ばれるグループを形成する。そして、同一のピコネットに属する電子機器間で相互に通信することが可能である。同一のピコネットには多くの電子機器が同時に属することができる。また、1 台の通信装置が同時に複数のピコネットに属することも可能である。このため、携帯型電話機を始め、パーソナルコンピュータ、PDA (Personal Digital Assistant) と呼ばれるハンドヘルドコンピュータ、プリンタ、音楽プレーヤ等の様々な機器を互いに接続する通信方式として注目されている。

以下、無線通信部 24 は上記 Bluetooth 規格に準じた通信ユニットであり、無線通信部 24 及びアンテナ 25 を利用して実行される無線通信 (無線通信リンク A を介した無線通信) は、Bluetooth 規格に準じた 2.4GHz 帯の電波により行われるものとして説明する。

赤外線通信部 26 は、エンコーダ、デコーダ等を内蔵しており、赤外線受発光ユニット 27 に接続されている。赤外線通信部 26 は、CPU 21 から入力された信号を変換して赤外線受発光ユニット 27 へ出力する。

赤外線受発光ユニット 27 は、LED (Light Emitting Diode) やフォトセ

ンサ等を内蔵し、赤外線通信部 2 6 から入力された信号をもとに内蔵する L E D を発光させ、赤外線信号として通信装置 3 へ向けて出力する。

また、赤外線受発光ユニット 2 7 は、内蔵するフォトセンサによって通信装置 3 からの赤外光を受光すると、受光パターンを所定の信号に変換して赤外線通信部 2 6 へ出力する。さらに、赤外線通信部 2 6 は、赤外線受発光ユニット 2 7 から入力される信号を変換して、CPU 2 1 へ出力する。

インターフェース部 2 8 は、通信装置 2 と、通信装置 2 の外部の電子機器とを接続するためのインターフェースであって、コネクタ等を備えている。ここで、インターフェース部 2 8 に接続される電子機器 4 としては、例えば、携帯型電話機やパーソナルコンピュータ、PDA 等が挙げられるが、特に限定されるものではない。また、通信装置 2 は、図示しないリチウムイオン電池やニッケルカドミウム電池等の二次電池、もしくは乾電池等を内蔵し、これらの電池を電源として動作するが、通信装置 2 に電池を内蔵せずに、インターフェース部 2 8 を介して通信装置 2 へ電源が供給される構成としても良い。

さらに、通信装置 2 が有する入力部 2 3 に代えて、インターフェース部 2 8 に接続された機器が具備する入力装置を用いる構成としても良い。この場合、CPU 2 1 は、インターフェース部 2 8 に接続された機器から入力される信号に従って動作すれば良く、入力部 2 3 を備えていなくても良い。

次いで、通信装置 3 の構成について説明する。

通信装置 3 は、CPU 3 1、メモリ 3 2、入力部 3 3、無線通信部 3 4、アンテナ 3 5、赤外線通信部 3 6、赤外線受発光ユニット 3 7、及びインターフェース部 3 8 の各部を備えて構成される。

ここで、上記メモリ 3 2、入力部 3 3、無線通信部 3 4、アンテナ 3 5、赤外線通信部 3 6、赤外線受発光ユニット 3 7、及びインターフェース部 3 8 の各部は、通信装置 2 が有するメモリ 2 2、入力部 2 3、無線通信部 2 4、アンテナ 2 5、赤外線通信部 2 6、赤外線受発光ユニット 2 7、及びインターフェース部 2 8 の各部と同一の構成によってなるものであり、説明を省略する。

CPU 3 1 は、入力部 3 3 における指示操作に従って、メモリ 3 2 に格納さ

れたシステムプログラムを読み出して実行し、通信装置 3 の各部を駆動制御する。

具体的には、CPU 31 は、メモリ 32 内のプログラムに従って、無線通信部 34 を制御し、通信装置 2 との間に無線通信リンク A を確立する。

- 5     続いて CPU 31 は、赤外線通信部 36 及び赤外線受発光ユニット 37 によって赤外線通信リンク B を確立する。そして、CPU 31 は、通信装置 2 が有する赤外線受発光ユニット 27 から発せられた赤外線信号を赤外線受発光ユニット 37 によって受光し、通信装置 2 から送信された暗号化に関する各種情報を受信する。
- 10    ここで、CPU 31 は、通信装置 2 から送信された各種情報をメモリ 32 内に格納するとともに、該情報を、赤外線通信部 36 及び赤外線受発光ユニット 37 を介して通信装置 2 へ送信する。そして、通信装置 2 が有するアンテナ 25 から出力された無線信号を受信し、受信した信号が無線通信リンク A 及び赤外線通信リンク B の切断を要求している場合は、通信装置 2 との間の無線通信
- 15    リンク A 及び赤外線通信リンク B を切断する。

次に、本実施の形態の動作を説明する。

- 図 3 は、本第 1 の実施の形態における通信システム 1 の動作を示すフローチャートである。この内、左側は、アクセス要求側の装置、すなわち通信装置 2
- 20    の動作 (S11~S19) を示し、右側はアクセス受信側の装置、すなわち通信装置 3 の動作 (S21~S29) を示す。なお、図中、実線矢印で示す信号は、無線通信リンク A (図 1) を介して送受信される上記 Bluetooth 規格に準じた無線信号であり、破線矢印で示す信号は、赤外線通信リンク B (図 1) を介して送受信される赤外線信号である。

- 25    まず、図 3 の左側に示すように、CPU 21 は、入力部 23 からの指示入力に従って動作を開始し、通信装置 3 に対して接続を求める接続要求信号を生成して、無線通信部 24 によって通信装置 3 へ送信させる (ステップ S11)。

CPU 31 は、入力部 33 からの指示入力によって動作を開始し、無線通信部 34 によって通信装置 2 から送信される無線信号を受信可能な状態に移行す

る。そして、無線通信部 2 4 から送信された接続要求を無線通信部 3 4 によって受信すると（ステップ S 2 1）、接続の確認となる接続確認信号を生成し、無線通信部 3 4 によって送信させる（ステップ S 2 2）。

CPU 2 1 は、CPU 3 1 の制御により無線通信部 3 4 から送信された接続確認信号を無線通信部 2 4 によって受信すると（ステップ S 1 2）、メモリ 2 2 の転送諸元情報格納領域 1 0 2 に格納された転送諸元情報を読み出して、赤外線通信部 2 6 及び赤外線受発光ユニット 2 7 によって、赤外線信号として通信装置 3 へ送信させる（ステップ S 1 3）。

CPU 3 1 は、通信装置 2 の赤外線通信部 2 6 により赤外線信号として送信された転送諸元情報を、赤外線通信部 3 6 によって受信すると（ステップ S 2 3）、メモリ 3 2 の転送諸元情報格納領域 1 0 2 に格納された転送諸元情報を読み出して、赤外線通信部 3 6 によって送信させる（ステップ S 2 4）。

CPU 2 1 は、通信装置 3 から送信された転送諸元情報を赤外線通信部 2 6 によって受信すると（ステップ S 1 4）、メモリ 2 2 内の原始暗号化情報格納領域 1 0 1 に格納されている原始暗号化情報を読み出して、赤外線通信部 2 6 によって通信装置 3 へ送信させる（ステップ S 1 5）。

CPU 3 1 は、通信装置 2 から送信された原始暗号化情報を受信すると（ステップ S 2 5）、受信した原始暗号化情報をメモリ 3 2 内の原始暗号化情報格納領域 1 0 1 に記憶させる（ステップ S 2 6）。なお、ここで、予めメモリ 3 2 の原始暗号化情報格納領域 1 0 1 に格納されていた原始暗号化情報については、新たに受信した原始暗号化情報により上書きされるものとしても良いし、或いは、新たに受信した原始暗号化情報とは異なる領域に保存されるものとしても良い。

続いて、CPU 3 1 は、ステップ S 2 5 で受信し、メモリ 3 2 内の原始暗号化情報格納領域 1 0 1 に記憶した原始暗号化情報を、赤外線通信部 3 6 によって通信装置 2 へ送信する（ステップ S 2 7）。

CPU 2 1 は、通信装置 3 から送信された原始暗号化情報を受信すると（ステップ S 1 6）、受信した原始暗号化情報と、メモリ 2 2 の原始暗号化情報格納領域 1 0 1 に格納されている原始暗号化情報とを照合し、一致することを確認

する（ステップS 17）。

すなわち、ステップS 15で通信装置3へ送信した原始暗号化情報と、通信装置3から送信された原始暗号化情報とが一致することを確認することにより、ステップS 15、S 16、S 25、S 26における原始暗号化情報の送受信が  
5 問題なく実行されたことを確認する。

そして、CPU 21は、通信の切断を要求する切断要求信号を生成して、無線通信部24によって通信装置3へ送信させる（ステップS 18）。

CPU 31は、通信装置2から送信された切断要求信号を無線通信部34によって受信すると（ステップS 28）、切断要求の受信を確認する切断確認信号  
10 を生成して、無線通信部34によって通信装置2へ送信させ（ステップS 29）、本処理を終了する。

また、CPU 21は、通信装置3から送信された切断確認信号を無線通信部24によって受信すると（ステップS 19）、本処理を終了する。

以上の図3に示す処理によって、通信装置2が有するメモリ22と、通信装置3が有するメモリ32とは、予めメモリ22内の原始暗号化情報格納領域1  
15 01に格納されていた原始暗号化情報を格納した状態になる。

図3に示す処理においては、転送諸元情報および原始暗号化情報が、赤外線通信リンクB（図1）を介して送受信される。

一般に、赤外線信号による無線通信を行う場合、通信を行う電子機器が互いに近接しており、かつ、互いの電子機器が有する赤外線受発光部が対向していることが必要である。特に、互いの電子機器が有する赤外線受発光部は、比較的狭い立体角に収まるように対向していなければならず、無関係な電子機器により傍受される可能性は低く、セキュリティ上の懸念は小さいものである。

しかしながら、以下に述べる暗号化を施すことにより、赤外線通信リンクB  
25 を介した通信におけるセキュリティ上の信頼性をより確実なものとすることができる。

図4Aには、暗号化を施す際の赤外線通信におけるプロトコル構成を示す階層モデルを図示する。また、図4Bには、赤外線通信におけるデータユニットの構成を模式的に示す。



一般に、赤外線通信においては、データリンク層、リンクマネージメント層、トランスポート層における互換性を保持していれば、それより上位の階層におけるサービス・データ・ユニットを暗号化しても、プロトコル互換性を保つことができる。従って、図4Aに示すように、トランスポート層よりも上位の層を暗号化層とし、さらにその上位層を、前述の転送諸元情報や原始暗号化情報を交換するセキュリティデータ交換プロトコル層とすれば、プロトコル互換性を保ちながら、転送される情報の秘匿性を保つことができる。

具体的には、図4Bに示すように、LAP（データリンク層）、LMP（リンクマネージメント層）、及びTP（トランスポート層）のプロトコルデータユニットに続くサービス・データ・ユニットを暗号化すれば良い。

従って、通信装置2及び通信装置3の双方において、赤外線通信リンクBを介して送受信する信号の暗号化及び復号を行うことにより、図3に示す処理で送受信される転送諸元情報や原始暗号化情報の秘匿性をより確実なものとすることができる。

図5は、図3に示す処理の実行後における通信装置2の動作を示すフローチャートである。

この図5に示す処理において、通信装置2は、Bluetooth規格により規定されるMasterのデバイスとして動作する。また、図5に示す処理において送受信される無線信号は、Bluetooth規格に準じた2.4GHz帯の無線信号である。

まず、CPU21は、入力部23から入力される指示に従って動作を開始し、無線通信部24を制御してPage Scan動作を実行し、Bluetooth規格に準じた通信が可能な通信装置を検出する（ステップS41）。

そして、接続可能な通信装置を検出した場合は、CPU21によるPage Scan動作に応じて検出した装置から送信された情報を受信し（ステップS42）、受信した情報と、メモリ22内の原始暗号化情報格納領域101に格納されている原始暗号化情報との照合を行う（ステップS43）。

ここで、通信装置2が通信装置3を検出した場合、通信装置3は、メモリ22内の原始暗号化情報格納領域101に格納されている原始暗号化情報を既に保持しているため、Page Scan動作に応じて原始暗号化情報に従って暗号化され

た情報を送信する。また、通信装置 2 及び通信装置 3 とは無関係な通信装置が検出された場合は、この無関係な通信装置からは、Page Scan 動作に応じて通常の無線信号が送信される。従って、ステップ S 4 3 における照合により、ステップ S 4 1 で検出した通信装置が通信装置 3 であるか否かを判別できる。

- 5     ステップ S 4 3 における照合の結果、ステップ S 4 2 で受信した無線信号が原始暗号化情報とは無関係であった場合は（ステップ S 4 4 ; No）、CPU 2 1 は、検出した通信装置との接続を拒否し（ステップ S 4 5）、本処理を終了する。

また、ステップ S 4 3 での照合により、ステップ S 4 2 で受信した無線信号  
10   が原始暗号化情報に適合した場合は（ステップ S 4 4 ; Yes）、CPU 2 1 は、検出した通信装置との間で、原始暗号化情報格納領域 1 0 1 内の原始暗号化情報により暗号化された無線信号の送受信を開始する（ステップ S 4 6）。

なお、原始暗号化情報格納領域 1 0 1 に格納された原始暗号化情報により暗号化された情報は、該原始暗号化情報をもとに復号できる。このため、CPU  
15   2 1 は、無線通信部 2 4 により送信する情報を暗号化するとともに、無線通信部 2 4 により受信した情報を復号する。

そして、CPU 2 1 は、検出した通信装置との間のネゴシエーションが終了してからアプリケーションでの使用を許可する（ステップ S 4 7）。

その後、CPU 2 1 は、通信装置 2、もしくはインターフェース部 2 8 に接  
20   続された電子機器 4 上で実行されるアプリケーションプログラムの要求に応じて、暗号化された無線信号を送受信する処理を実行し（ステップ S 4 8）、入力部 2 3 からの指示入力によって本処理を終了する。

以上のように、本発明の第 1 の実施の形態によれば、Bluetooth 規格に準じた無線通信を行う無線通信部 2 4 及びアンテナ 2 5 と、赤外線信号を用いた無線  
25   通信を行う赤外線通信部 2 6 及び赤外線受発光ユニット 2 7 とを備える通信装置 2 と、通信装置 2 と同一構成によってなる通信装置 3 との間において、予め赤外線通信によって原始暗号化情報を転送し、その後、転送した原始暗号化情報に基づいて暗号化された情報を、Bluetooth 規格に準じた無線通信で送受信する。

これにより、高い秘匿性を保ちながら、Bluetooth 規格に準じた利便性の高い通信を行うことができる。

すなわち、Bluetooth 規格に準じた無線通信を利用した場合、互いの通信装置を近接させるだけでピコネットを形成して通信を開始できる。また、通信中の  
5 各通信機器は、同時に他の通信装置との間においてピコネットを形成することができ、フレキシブルな通信を行うことができる。さらに、ピコネットを形成する通信装置は、互いに所定の距離以内に近接していれば良く、位置が拘束されることが少ない。その反面、Bluetooth 規格に準じた無線通信では、特定の通信装置に対してのみ情報を送信することが難しく、誤って無関係な通信装置に  
10 受信されてしまう可能性が否定できない。

しかしながら、上記第 1 の実施の形態における通信システム 1 によれば、予め通信装置 2 と通信装置 3 との間で、赤外線通信によって原始暗号化情報を転送することにより、無関係な通信装置に影響されることなく原始暗号化情報を共有し、この原始暗号化情報を用いて暗号化された情報を、Bluetooth 規格に準  
15 じた無線通信で送受信する。従って、セキュリティ上の信頼性を確保しながら、利便性の高い無線通信を行うことができる。

なお、上記実施の形態においては、通信装置 2 と通信装置 3 とは、Bluetooth 規格に準じた無線通信リンク A を介して無線通信を行うものとしたが、本発明はこれに限定されるものではなく、仕様や規格が公開され、或いは広く普及し  
20 て互換性が保たれている無線通信方式に対しても適用可能であり、上記の通信システム 1 と同様の効果を奏するものである。

さらに、携帯型電話機や PDA、パーソナルコンピュータ、プリンタ、音楽プレーヤ等の各種電子機器に本発明を適用する場合は、図 1 に示したような通信装置 2 及び通信装置 3 に対して電子機器 4、5 が接続される構成に限らず、  
25 上記各種電子機器に、通信装置 2、3 の機能を内蔵させることも勿論可能である。

また、上記第 1 の実施の形態においては、通信装置 2 及び通信装置 3 はいずれも入力部 23、33 を具備しており、これら入力部 23、33 における指示入力によって図 3 に示す処理を開始するものとしたが、必ずしも入力部 23、

33を備える構成でなくても良い。以下、この場合について第2の実施の形態として説明する。

第2の実施の形態：

- 5 図6は、本発明の第2の実施の形態における通信システム10の構成を示すブロック図である。

同図に示すように、通信システム10は、通信装置2と、通信装置3aとによって構成される。通信システム10は、通信装置3aが有するメモリ61およびスイッチ62を除いては、上記第1の実施の形態における通信システム1  
10 と同様の構成によってなるものであり、共通部分については同符号を付して説明を省略する。

スイッチ62は、1個もしくは複数のスイッチを備えており、操作される毎に操作信号を生成してCPU31へ出力する。

- 図7は、メモリ61の内部構成を模式的に示す図である。同図に示すように、  
15 メモリ61内には、原始暗号化情報格納領域103及び転送諸元情報格納領域102が設けられており、転送諸元情報格納領域102には製品情報、固有機能情報、使用者情報、シリアルNo.等の転送諸元情報が格納されている。一方、原始暗号化情報格納領域103には、事前に原始暗号化情報は格納されていない。

- 20 上記第1の実施の形態で説明した通信システム1では、図3に示す処理において、通信装置2から通信装置3へ原始暗号化情報が転送され、メモリ22の原始暗号化情報格納領域101に格納されていた原始暗号化情報が、メモリ32の原始暗号化情報格納領域101に格納される。

- 本第2の実施の形態における通信システム10では、通信装置2から通信装  
25 置3aへ原始暗号化情報が転送されると、転送された原始暗号化情報はメモリ61の原始暗号化情報格納領域103へ格納される。従って、通信装置3aは、上記通信装置3と同様に動作することができる。

また、上記第1の実施の形態で説明した通信システム1では、通信装置2が有する入力部23および通信装置3が有する入力部33における指示入力によ

り、図 3 に示す処理が開始されるものとした。

本第 2 の実施の形態における通信システム 10 では、通信装置 2 が有する入力部 23 における指示入力、及び、通信装置 3a が有するスイッチ 62 のスイッチ操作によって、図 3 に示す処理と同様の処理が実行される。

5     すなわち、通信装置 3a は、入力手段としてスイッチ 62 のみを備える装置であるが、上記第 1 の実施の形態における通信装置 3 に代えて、通信装置 2 によるアクセスを受信する動作のみを行う装置として使用可能である。また、通信装置 2 に代えてアクセス要求側の装置として利用しないため、メモリ 61 の原始暗号化情報格納領域 103 には予め原始暗号化情報を格納する必要がない。

10    従って、本第 2 の実施の形態における通信システム 10 は、入力スイッチ 62 のみを有する通信装置 3a を用いて、上記第 1 の実施の形態と同様の効果を奏するものである。これにより、Bluetooth 規格に準じた無線通信において、Slave のデバイスとしてのみ機能する装置には、入力手段としては単なるスイッチを備えるだけで、通信システム 1 と同様の効果を得ることができる。

15     以上に記載したように、本発明の第 1 の側面による通信装置によれば、送信される情報は、第 2 の通信手段によって送信された暗号化鍵情報を受信した通信装置でのみ受信可能となる。これにより、第 1 の通信手段による無線通信について、セキュリティ上の信頼性を確保することができる。特に、第 1 の通信  
20    手段による無線通信が、例えばブルートゥース規格のように、仕様や規格が公開され、或いは広く普及して互換性が保たれている無線通信方式に準じたものである場合は、無関係な通信装置により受信されてしまう可能性が否定できない。しかしながら、本発明を適用すれば、通信の相手を、第 2 の通信手段によって送信される暗号化鍵情報を受信した通信装置のみに限定できる。従って、  
25    通信相手の装置との位置関係が比較的自由である等、無線通信の利便性を損なうことなく、情報の秘匿性を保持し、セキュリティ上の信頼性を確保することができる。

また、鍵情報保持手段に保持された暗号化鍵情報と同一の暗号化鍵情報を保持していない外部の通信装置に対しては、通信拒否手段により、第 1 の通信手

段による無線信号の送受信を拒否するような構造とすれば、通信の相手となる通信装置を厳格に限定し、情報の秘匿をより確実に保持することができる。

さらに、第1の通信手段はブルートゥース規格に準じた通信方式により無線信号を送受信するものであり、前記第2の通信手段は、赤外線信号を用いた通信方式により無線信号を送受信するようにすれば、広く仕様が公開され、利便性に富む一方、確実な情報秘匿が困難なブルートゥース (Bluetooth) 規格の無線通信において、情報の秘匿性を確保することができる。特に、第2の通信手段に赤外線信号を用いた通信方式を利用するので、第2の通信手段の小型化、軽量化、低コスト化および省電力化が可能であり、容易に実現可能である。また、赤外線信号を用いた通信方式では、通信装置は互いに近接し、かつ所定の立体角以内で対向する必要があるので、情報の秘匿性をより一層高めることができる。

また、本発明の上記通信システムまたは通信方法によれば、送信側装置により送信される情報は受信側装置でのみ受信することができる。これにより、送信側装置が有する第1の通信手段を用いた通信システム内の無線通信について、セキュリティ上の信頼性を確保することができる。特に、第1の通信手段による無線通信が、例えばブルートゥース規格のように、仕様や規格が公開され、或いは広く普及して互換性が保たれている無線通信方式に準じたものである場合は、無関係な通信装置により受信されてしまう可能性が否定できない。しかしながら、本発明を適用すれば、通信の相手を、第2の通信手段によって送信される暗号化鍵情報を保持する受信側装置のみに限定できる。従って、互いの装置の位置関係が比較的自由である等、無線通信の利便性を損なうことなく、情報の秘匿性を保持し、セキュリティ上の信頼性を確保することができる。

また、送信側装置は、鍵情報保持手段に保持された暗号化鍵情報と同一の暗号化鍵情報が、受信側装置が有する受信鍵情報保持手段に保持されていない場合に、通信拒否手段によって、第1の通信手段による無線信号の送受信を拒否するようにすれば、通信の相手となる通信装置をより厳格に限定し、情報の秘匿をより確実に保持することができる。

さらに、前記送信側装置が有する第1の通信手段と、前記受信側装置が有す

- る暗号化情報受信手段とは、ブルートゥース規格に準じた通信方式により無線信号を送受信するものであって、前記送信側装置が有する前記第2の通信手段と、前記受信側装置が有する鍵情報受信手段とは、赤外線信号を用いた通信方式により無線信号を送受信するようにすれば、広く仕様が公開され、利便性に富む一方、確実な情報秘匿が困難なブルートゥース（Bluetooth）規格の無線通信において、情報の秘匿性を確保することができる。特に、第2の通信手段と鍵情報受信手段とは赤外線信号を用いた通信方式を利用するので、第2の通信手段および鍵情報受信手段の小型化、軽量化、低コスト化および省電力化が可能であり、容易に実現可能である。また、赤外線信号を用いた通信方式では、送信側装置と受信側装置とは互いに近接し、かつ所定の立体角以内で対向する必要があるため、情報の秘匿性をより一層高めることができる。
- また、送信側装置が有する鍵情報送信制御手段は、暗号化鍵情報を暗号化して第2の通信手段によって送信させるようにすれば、暗号化鍵情報を送信する際の情報の漏洩をより確実に防止できる。これにより、セキュリティ上の信頼性をより一層高めることができる。

#### 産業上の利用可能性

- 本発明は、複数の電子機器間で無線通信によってデータを送受信する種々の通信システム、特に、情報の秘匿性を保持しセキュリティ上の信頼性を確保することが要求される通信システムに用いるのに適している。

## 請 求 の 範 囲

1. 無線信号を送受信する第1の通信手段と、  
この第1の通信手段とは異なる通信方式により信号を送受信する第2の通信  
5 手段と、  
暗号化鍵情報を保持する鍵情報保持手段と、  
この鍵情報保持手段に保持された暗号化鍵情報を、前記第2の通信手段によ  
って他の通信装置へ送信させる鍵情報送信制御手段と、  
前記鍵情報保持手段に保持された暗号化鍵情報をもとに情報を暗号化して、  
10 前記第1の通信手段によって送信させる通信制御手段と  
を備える通信装置。  
2. 前記鍵情報保持手段に保持された暗号化鍵情報と同一の暗号化鍵情報を  
保持していない外部の通信装置に対しては、前記第1の通信手段による無線信  
号の送受信を拒否する通信拒否手段をさらに備える請求の範囲第1項記載の通  
15 信装置。  
3. 前記第1の通信手段はブルートゥース規格に準じた通信方式により無線  
信号を送受信するものであって、前記第2の通信手段は、赤外線信号を用いた  
通信方式により無線信号を送受信する請求の範囲第1項または第2項記載の通  
信装置。  
20 4. 前記赤外線信号を用いた通信方式におけるプロトコルデータユニットは、  
データリンク層、リンクマネージメント層、トランスポート層に続いて、暗号  
化されたサービスデータユニットを有する請求の範囲第3項記載の通信装置。  
5. 送信側装置と受信側装置とを備えてなる通信システムであって、  
前記送信側装置は、  
25 無線信号を送受信する第1の通信手段と、  
この第1の通信手段とは異なる通信方式により信号を送受信する第2の通信  
手段と、  
暗号化鍵情報を保持する鍵情報保持手段と、  
この鍵情報保持手段に保持された暗号化鍵情報を、前記第2の通信手段によ



って前記受信側装置へ送信させる鍵情報送信制御手段と、

前記鍵情報保持手段に保持された暗号化鍵情報をもとに情報を暗号化して、  
前記第 1 の通信手段によって前記受信側装置へ送信させる通信制御手段とを備え、

5 前記受信側装置は、

前記送信側装置が有する第 2 の通信手段により送信された暗号化鍵情報を受信する鍵情報受信手段と、

この鍵情報受信手段により受信された暗号化鍵情報を保持する受信鍵情報保持手段と、

10 前記送信側装置が有する第 1 の通信手段により送信された情報を受信する暗号化情報受信手段とを備える

通信システム。

6. 前記送信側装置は、前記鍵情報保持手段に保持された暗号化鍵情報と同一の暗号化鍵情報が、前記受信側装置が有する受信鍵情報保持手段に保持されていない場合に、前記第 1 の通信手段による無線信号の送受信を拒否する通信拒否手段をさらに備える請求の範囲第 5 項記載の通信システム。

7. 前記送信側装置が有する第 1 の通信手段と、前記受信側装置が有する暗号化情報受信手段とは、ブルートゥース規格に準じた通信方式により無線信号を送受信するものであって、

20 前記送信側装置が有する前記第 2 の通信手段と、前記受信側装置が有する鍵情報受信手段とは、赤外線信号を用いた通信方式により無線信号を送受信する請求の範囲第 5 項または第 6 項記載の通信システム。

8. 前記送信側装置が有する鍵情報送信制御手段は、前記暗号化鍵情報を暗号化して前記第 2 の通信手段によって送信させる請求の範囲第 5 項または第 6  
25 項記載の通信システム。

9. 無線信号を送受信する第 1 の通信手段と、この第 1 の通信手段とは異なる通信方式により信号を送受信する第 2 の通信手段とを有する送信側装置と、受信側装置とを備えてなる通信システムにおける通信方法であって、

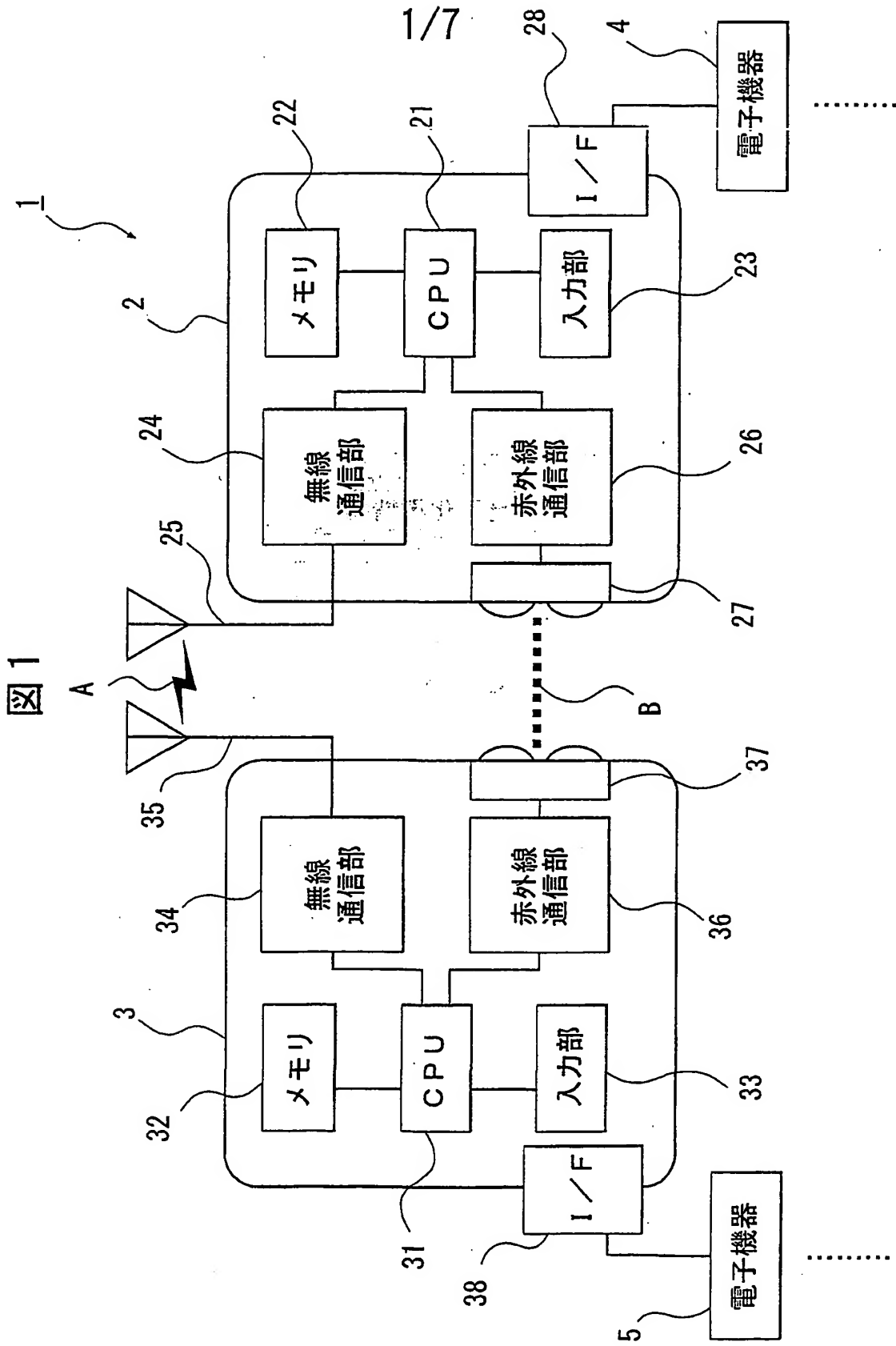
前記送信側装置により、暗号化鍵情報を前記第 2 の通信手段によって前記受

信側装置へ送信する工程と、

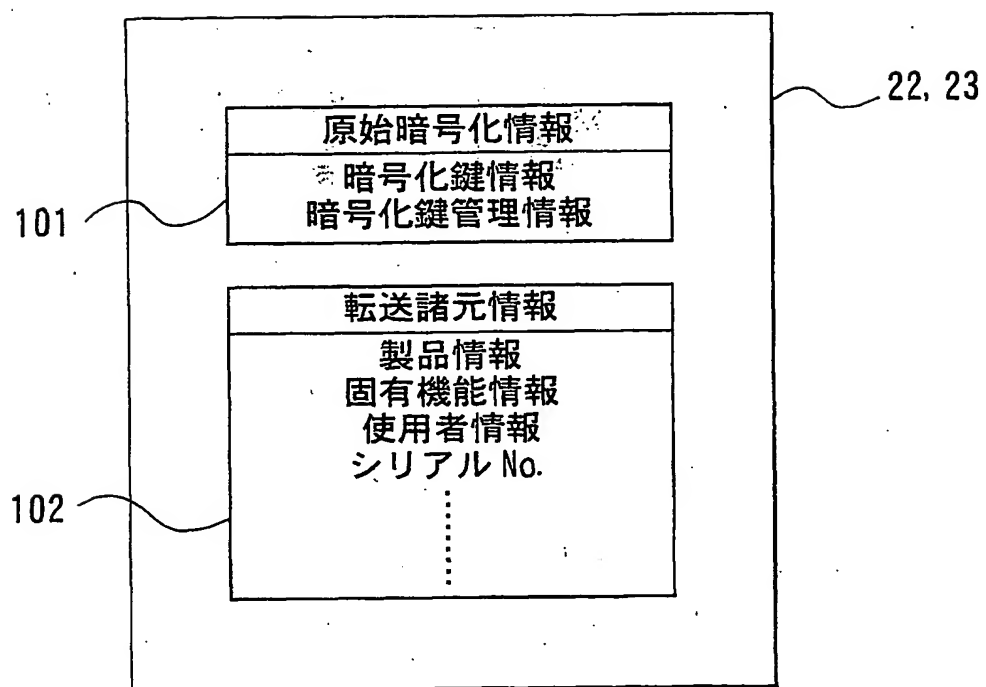
前記受信側装置により、前記送信側装置が有する第 2 の通信手段により送信された暗号化鍵情報を受信して記憶する工程と、

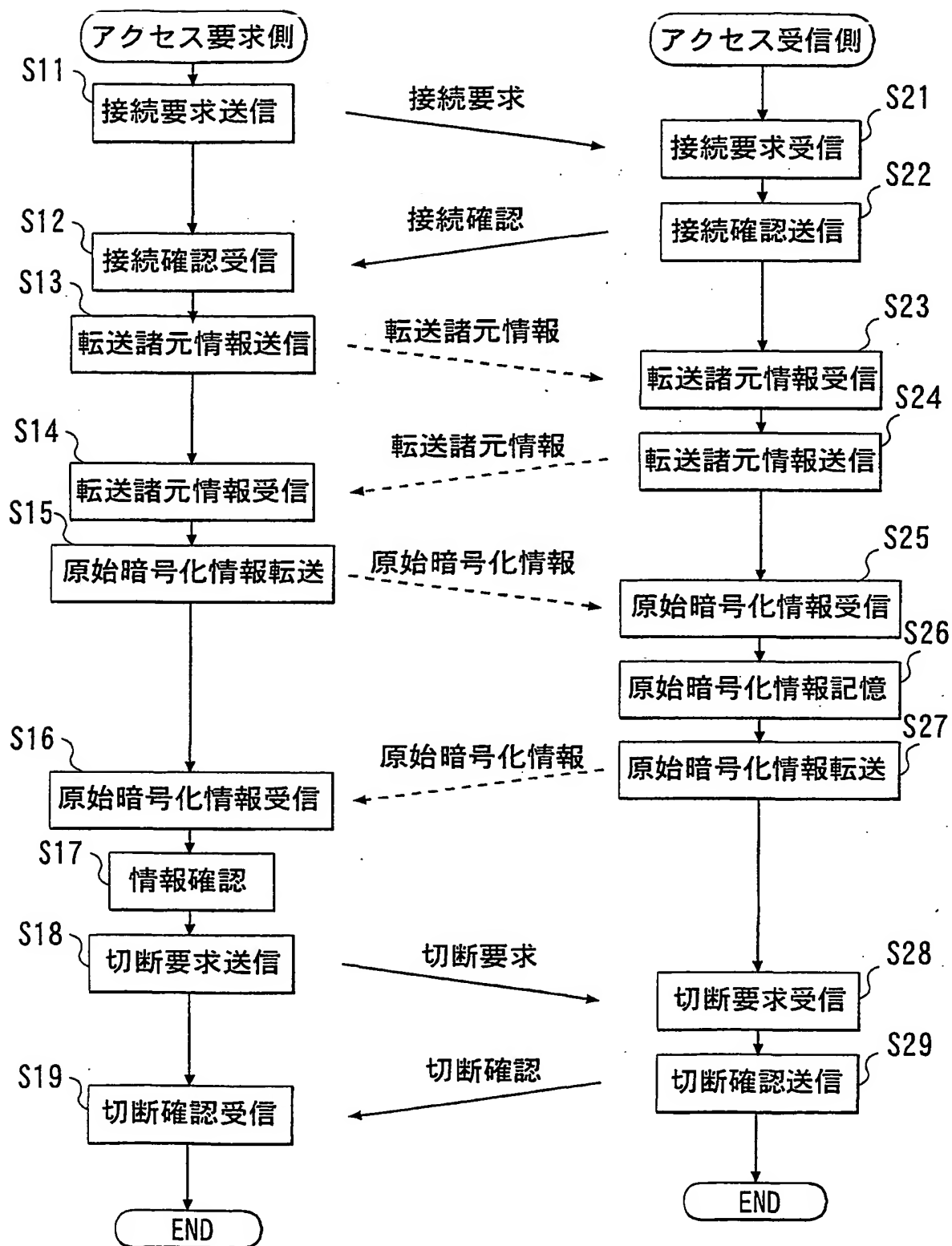
前記送信側装置により、前記暗号化鍵情報をもとに情報を暗号化して、前記

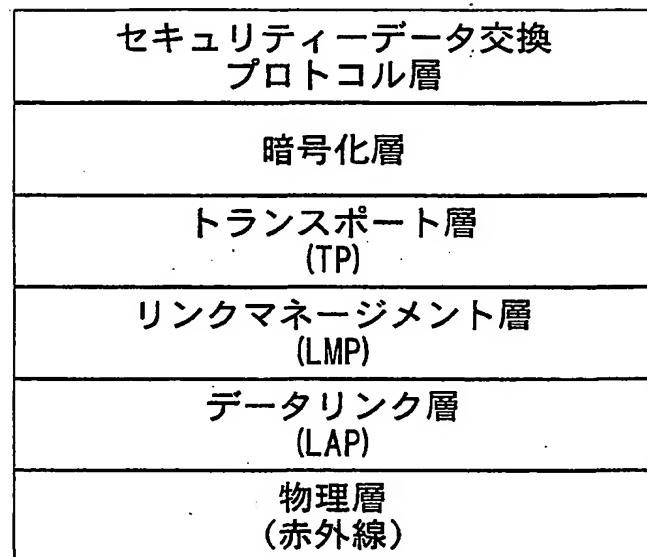
- 5 第 1 の通信手段によって前記受信側装置へ送信する工程と  
を含む通信方法。



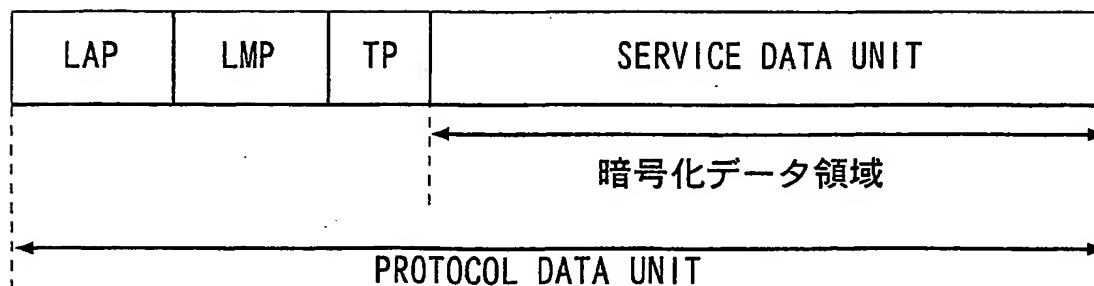
2/7  
図 2



3/7  
図 3

4/7  
図 4A

## 図 4B



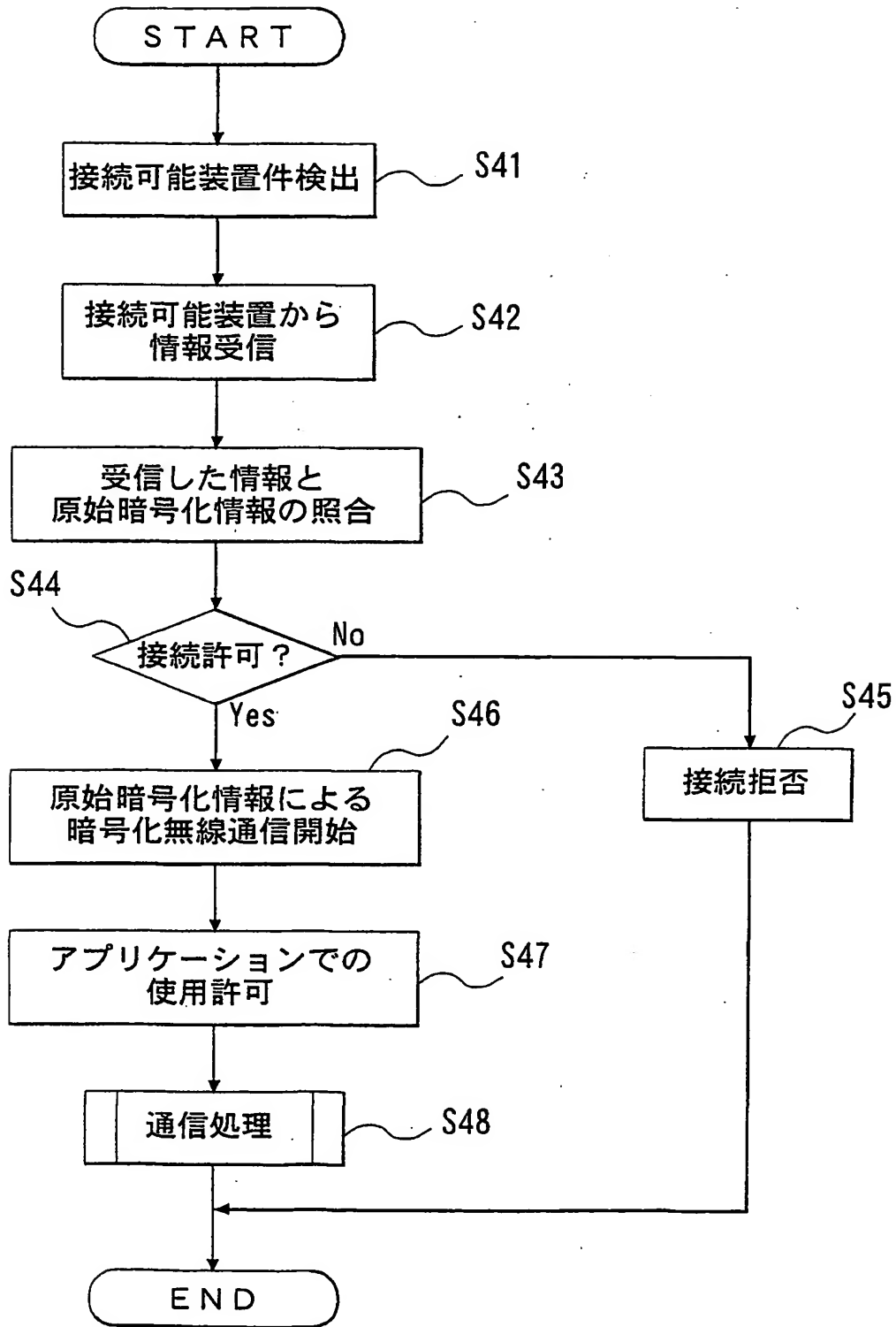
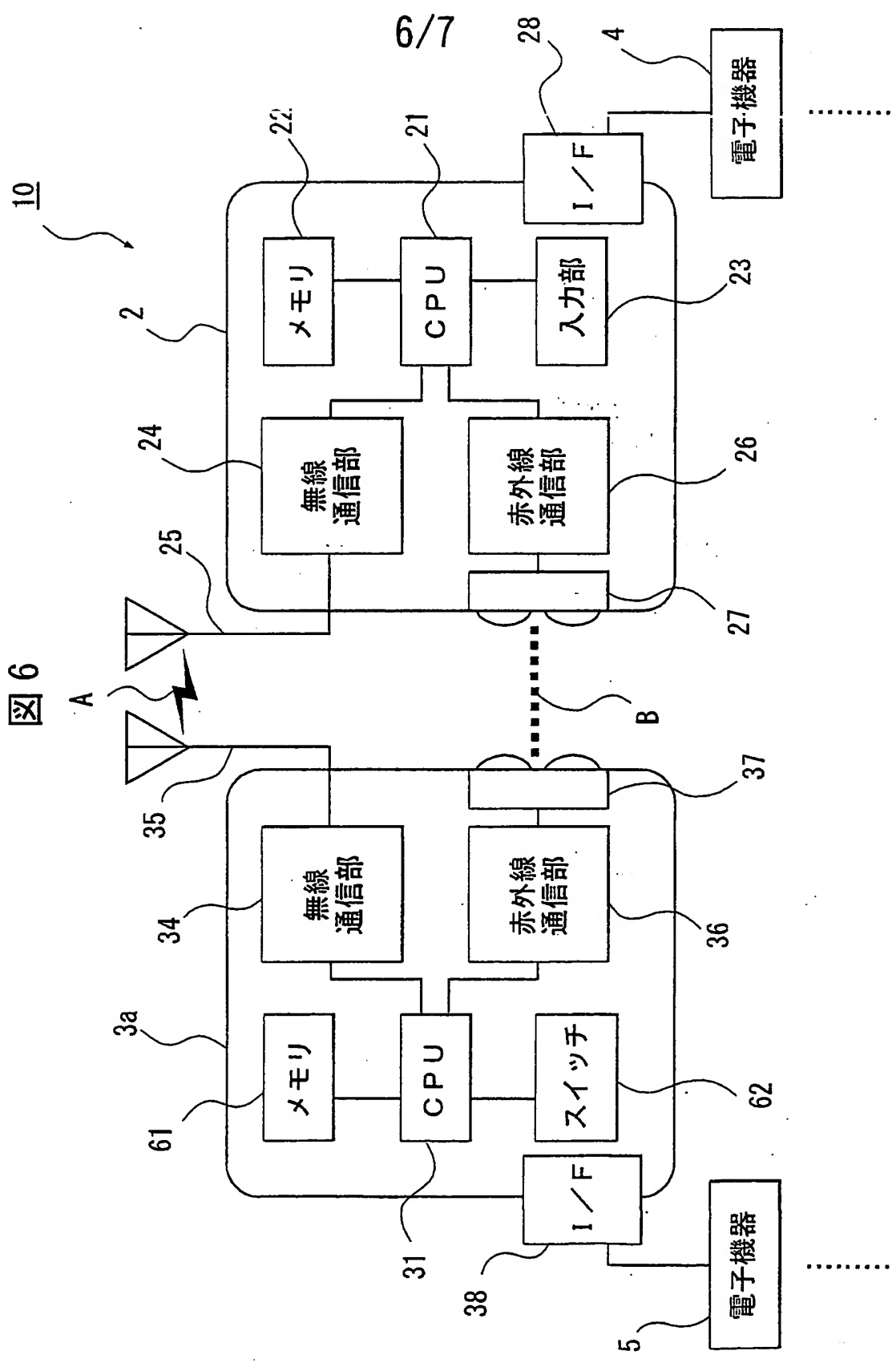
5/7  
図 5

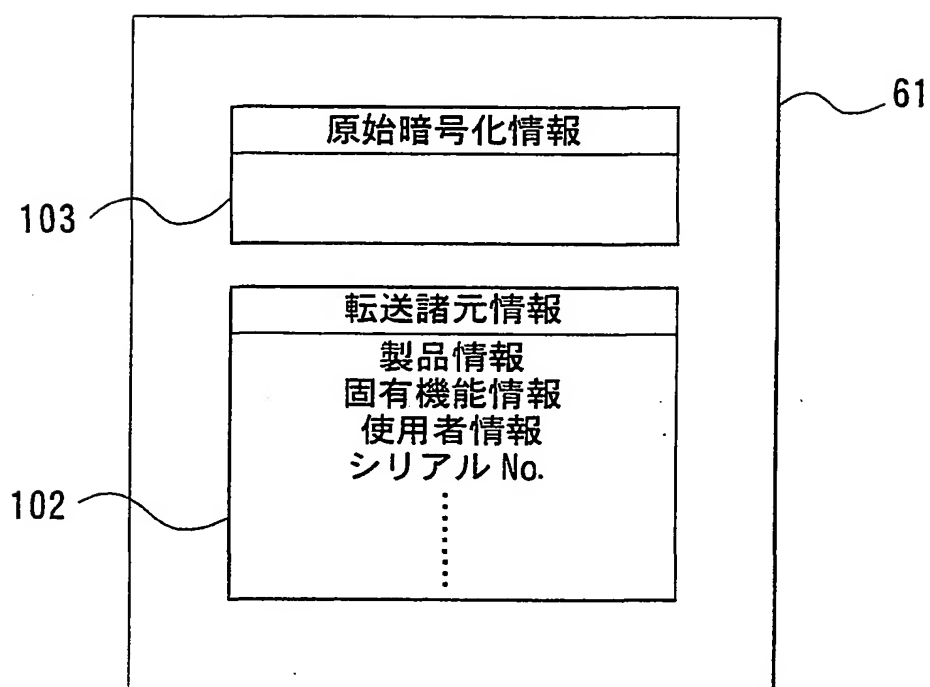
図 6





7/7

図 7



## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/04441

A. CLASSIFICATION OF SUBJECT MATTER  
Int.Cl<sup>7</sup> H04L12/28

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl<sup>7</sup> H04L12/28

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1926-2001 Kokai Jitsuyo Shinan Koho 1971-2001

Toroku Jitsuyo Shinan Koho 1994-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2000-224156 A (International Business Machines Corporation), 11 August, 2000 (11.08.00), columns 1 to 18; Figs. 1, 2 & EP 1024626 A1 & CA 2296223 A1 & CN 1262563 A & KR 2000057751 A	1-9
A	JP 11-150547 A (International Business Machines Corporation), 02 June, 1999 (02.06.99), & US 5930368 A & US 6067076 A & US 6072468 A & KR 98079782 A	1-9

☐ Further documents are listed in the continuation of Box C.☐ See patent family annex.

\* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T"

later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X"

document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y"

document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&amp;"

document member of the same patent family

Date of the actual completion of the international search  
17 August, 2001 (17.08.01)Date of mailing of the international search report  
28 August, 2001 (28.08.01)Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

## A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl<sup>7</sup> H04L12/28

## B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl<sup>7</sup> H04L12/28

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1926-2001年

日本国登録実用新案公報 1994-2001年

日本国公開実用新案公報 1971-2001年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

## C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	JP 2000-224156 A (インターナショナル・ビジネス・マシーンズ・コーポレーション) 11. 8月. 2000 (11. 08. 00), 第1-18欄, 第1, 2図 & EP 1024626 A1 & CA 2296223 A1 & CN 1262563 A & KR 2000057751 A	1-9
A	JP 11-150547 A (インターナショナル・ビジネス・マシーンズ・コーポレーション) 2. 6月. 1999 (02. 06. 99) & US 5930368 A & US 6067076 A & US 6072468 A & KR 98079782 A	1-9

☐ C欄の続きにも文献が列举されている。☐ パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの

「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」 口頭による開示、使用、展示等に言及する文献

「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&amp;」 同一パテントファミリー文献

国際調査を完了した日

17. 08. 01

国際調査報告の発送日

28.08.01

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

萩原 義則

5 X

8 2 2 4

電話番号 03-3581-1101 内線 3556